

IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND the claims in accordance with the following:

1. (CURRENTLY AMENDED) An information processing method in a center system, comprising:

receiving a first digital signature for specific data and data concerning a first user to be allowed to read said specific data, from a terminal of a second user;

confirming if an authority to give said first user permission to read said specific data is granted to said second user by comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said specific data; and

if it is judged that said first signature and said second signature are identical, performing a processing for enabling said first user to read said specific data.

2. (CURRENTLY AMENDED) The information processing method as set forth in claim 1, wherein said performing comprises transmitting hash data, which is registered in said data storage unit so as to correspond to said specific data, and which represents that an authority to read said specific data is granted to said first user, to a terminal of said first user.

3. (CURRENTLY AMENDED) The information processing method as set forth in claim 1, further comprising:

if it is judged that said first signature and said second signature are not identical, generating second hash data from said first digital signature;

confirming if said authority to give said first user said permission to read said specific data is granted to said second user by comparing the generated second hash data with hash data, which is registered in said data storage unit so as to correspond to said specific data; and executing a processing for enabling said first user to read said specific data.

4. (CURRENTLY AMENDED) The information processing method as set forth in claim 3,

wherein said executing comprises transmitting hash data, which is registered in said data storage unit so as to correspond to said specific data, and which represent that an authority to read said specific data is granted to said first user, to a terminal of said first user.

5. (CURRENTLY AMENDED) An access authority management method in a center system, comprising:

receiving a first digital signature for specific data from a terminal of a user;
confirming if an authority to update said specific data is granted to said user by
comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said specific data; and
if ~~it is judged that~~ said first digital signature and said second digital signature are identical, carrying out a setting to grant allow said user ~~an authority~~ to update said specific data.

6. (CURRENTLY AMENDED) The access authority management method as set forth in claim 5, further comprising:

if ~~it is judged that~~ said first digital signature and said second digital signature are not identical, generating first hash data from said first digital signature;
confirming if an authority to read said specific data is granted to said user by comparing said first hash data with second hash data, which is registered in said data storage unit so as to correspond to said specific data; and
if ~~it is judged that~~ said first hash data and said second hash data are identical, carrying out a setting to grant allow said user ~~an authority~~ to read said specific data.

7. (CURRENTLY AMENDED) The access authority management method as set forth in claim 6, further comprising transmitting an access denial notice to said terminal of said user, if ~~it is judged that~~ said first hash data and said second hash data are not identical.

8. (ORIGINAL) The access authority management method as set forth in claim 5, further comprising:

if data for updating said specific data is received from said terminal of said user, generating third hash data for the updated specific data;
transmitting said third hash data to said terminal of said user; receiving a third digital signature generated from said third hash data, from said terminal of said user; and
registering said updated specific data, said third hash data, and said third digital

signature into said data storage unit.

9. (CURRENTLY AMENDED) The access authority management method as set forth in claim 8, further comprising:

generating fourth hash data from said third digital signature before said registering; and
comparing said fourth hash data with said third hash data, and wherein said registering is executed if ~~it is judged that~~ said fourth hash data and said third hash data are identical.

10. (ORIGINAL) The access authority management method as set forth in claim 6, further comprising, if said authority to read said specific data is granted to said user, transmitting said specific data in a state where only reading is enabled, to said terminal of said user.

11. (CURRENTLY AMENDED) A data registration method in a center system, comprising:

if specific data is received from a user terminal, generate hash data for said specific data; transmitting said hash data to said user terminal; receiving a digital signature generated from said hash data; and
registering said specific data, said hash data and said digital signature into a data storage unit, and

wherein the registered hash and the registered digital signature is used to confirm if an authority to access said specific data is granted to an access requestor.

12. (CURRENTLY AMENDED) A data access method in a user system, comprising:
generating a digital signature from hash data, which is stored in a hash storage, for specific data;

transmitting an access request including said digital signature as data representing permission to update said specific data to a server; and

if said digital signature and a second digital signature, which is registered in said server, for said specific data are identical, receiving and displaying on a display device, said specific data in a state where updating is enabled, from said server.

13. (CURRENTLY AMENDED) The data access method as set forth in claim 12, further comprising, if said digital signature and said second digital signature, which is registered in said server, for said specific data are not identical, but hash data, which represents that an authority

to read said specific data is granted to said user, and which is generated from said digital signature, and second hash data, which is registered in said server, for said specific data are identical, receiving and displaying on a display device, said specific data in a state where only reading is enabled, from said server.

14. (CURRENTLY AMENDED) A computer-readable medium storing a program embodied on a computer-readable medium, said computer program comprising for controlling an apparatus by:

receiving a first digital signature for specific data and data concerning a first user to be allowed to read said specific data, from a terminal of a second user;

confirming if an authority to give said first user permission to read said specific data is granted to said second user by comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said specific data; and

if it is judged that said first signature and said second signature are identical, performing a processing for enabling said first user to read said specific data.

15. (CURRENTLY AMENDED) The computer-readable medium program as set forth in claim 14, wherein said performing comprises transmitting hash data, which is registered in said data storage unit so as to correspond to said specific data, and which represents that an authority to read said specific data is granted to said first user, to a terminal of said first user.

16. (CURRENTLY AMENDED) The computer-readable medium program as set forth in claim 14, further comprising:

if it is judged that said first signature and said second signature are not identical, generating second hash data from said first digital signature;

confirming if said authority to give said first user said permission to read said specific data is granted to said second user by comparing the generated second hash data with hash data, which is registered in said data storage unit so as to correspond to said specific data; and

executing a processing for enabling said first user to read said specific data.

17. (CURRENTLY AMENDED) The computer-readable medium program as set forth in claim 16, wherein said executing comprises transmitting hash data, which is registered in said data storage unit so as to correspond to said specific data, and which represents that an

authority to read said specific data is granted to said first user, to a terminal of said first user.

18. (CURRENTLY AMENDED) A computer-readable medium storing a program for an access authority management, said computer-program comprisingcontrolling an apparatus by: receiving a first digital signature for specific data from a terminal of a user; confirming if an authority to update said specific data is granted to said user by comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said specific data; and if it is judged that said first digital signature and said second digital signature are identical, carrying out a setting to grantallow said user an authority to update said specific data.

19. (CURRENTLY AMENDED) The computer-readable medium program as set forth in claim 18, further comprising:
if it is judged that said first digital signature and said second digital signature are not identical, generating first hash data from said first digital signature; confirming if an authority to read said specific data is granted to said user by comparing said first hash data with second hash data, which is registered in said data storage unit so as to correspond to said specific data; and if it is judged that said first hash data and said second hash data are identical, carrying out a setting to grantallow said user an authority to read said specific data.

20. (CURRENTLY AMENDED) The computer-readable medium program as set forth in claim 19, further comprising transmitting an access denial notice to said terminal of said user, if it is judged that said first hash data and said second hash data are not identical.

21. (CURRENTLY AMENDED) The computer-readable medium program as set forth in claim 18, further comprising:
if data for updating said specific data is received from said terminal of said user, generating third hash data for the updated specific data; transmitting said third hash data to said terminal of said user; receiving a third digital signature generated from said third hash data, from said terminal of said user; and registering said updated specific data, said third hash data, and said third digital signature into said data storage unit.

22. (CURRENTLY AMENDED) The computer-readable medium ~~program~~ as set forth in claim 21, further comprising:

generating fourth hash data from said third digital signature before said registering; and comparing said fourth hash data with said third hash data, and wherein said registering is executed if ~~it is judged that~~ said fourth hash data and said third hash data are identical.

23. (CURRENTLY AMENDED) The computer-readable medium ~~program~~ as set forth in claim 19, further comprising, if said authority to read said specific data is granted to said user, transmitting said specific data in a state where only reading is enabled, to said terminal of said user.

24. (CURRENTLY AMENDED) A center system, comprising:

~~means for receiving a unit that receives~~ a first digital signature for specific data and data concerning a first user to be allowed to read said specific data, from a terminal of a second user;

~~means for comparing a unit that confirms if an authority to give said first user permission to read said specific data is granted to said second user by comparing~~ the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said specific data; and

~~means for performing a unit that performs~~ a processing for enabling said first user to read said specific data, if ~~it is judged that~~ said first signature and said second signature are identical.

25. (CURRENTLY AMENDED) The center system as set forth in claim 24, wherein said ~~means for performing~~ unit that performs a processing comprises ~~means for transmitting~~ unit that transmits hash data, which is registered in said data storage unit so as to correspond to said specific data, and which represents that an authority to read said specific data is granted to said first user, to a terminal of said first user.

26. (CURRENTLY AMENDED) The center system as set forth in claim 24, further comprising:

~~means for generating~~ a unit that generates second hash data from said first digital signature, if ~~it is judged that~~ said first signature and said second signature are not identical;

~~means for~~ a unit that confirms if said authority to give said first user said permission to

read said specific data is granted to said second user by comparing the generated second hash data with hash data, which is registered in said data storage unit so as to correspond to said specific data; and

means for executing a unit that executes a processing for enabling said first user to read said specific data.

27. (CURRENTLY AMENDED) The center system as set forth in claim 26, wherein said means for executing a unit that executes a processing comprises means for transmitting a unit that transmits hash data, which is registered in said data storage unit so as to correspond to said specific data, and which represents that an authority to read said specific data is granted to said first user, to a terminal of said first user.

28. (CURRENTLY AMENDED) A center system, comprising:

means for receiving a unit that receives a first digital signature for specific data from a terminal of a user;

means for a unit that confirms if an authority to update said specific data is granted to said user by comparing the received first digital signature with a second digital signature, which is registered in a data storage unit so as to correspond to said specific data; and

means for carrying a unit that carries out a setting to grant allow said user an authority to update said specific data, if it is judged that said first digital signature and said second digital signature are identical.

29. (CURRENTLY AMENDED) The center system as set forth in claim 28, further comprising:

means for generating a unit that generates a first hash data from said first digital signature, if it is judged that said first digital signature and said second digital signature are not identical;

means for a unit that confirms if an authority to read said specific data is granted to said user by comparing said first hash data with second hash data, which is registered in said data storage unit so as to correspond to said specific data; and

means for carrying a unit that carries out a setting to grant allow said user an authority to read said specific data, if it is judged that said first hash data and said second hash data are identical.

30. (CURRENTLY AMENDED) The center system as set forth in claim 29, further comprising ~~means for transmittinga unit that transmitting~~ an access denial notice to said terminal of said user, if ~~it is judged that~~ said first hash data and said second hash data are not identical.

31. (CURRENTLY AMENDED) The center system as set forth in claim 28, further comprising:

~~means for generatinga unit that generates~~, if data for updating said specific data is received from said terminal of said user, third hash data for the updated specific data;

~~means for transmittinga unit that transmits~~ said third hash data to said terminal of said user;

~~means for receivinga unit that receives~~ a third digital signature generated from said third hash data, from said terminal of said user; and

~~means for registeringa unit that registers~~ said updated specific data, said third hash data, and said third digital signature into said data storage unit.

32. (CURRENTLY AMENDED) The center system as set forth in claim 31, further comprising:

~~means for generatinga unit that generates~~ a fourth hash data from said third digital signature before said registering; and

~~means for comparinga unit that compares~~ said fourth hash data with said third hash data, and wherein ~~means for registeringunit that registers~~ operates if ~~it is judged that~~ said fourth hash data and said third hash data are identical.

33. (CURRENTLY AMENDED) The center system as set forth in claim 29, further comprising ~~means for transmittinga unit that transmits~~ said specific data in a state where only reading is enabled, to said terminal of said user, if said authority to read said specific data is granted to said user.